Title (en)

Method for secure evaluation of a function applied to encrypted signals

Title (de)

Verfahren zur sicheren Auswertung einer Funktion, die auf verschlüsselte Signal angewendet wird

Title (fr)

Procédé d'évaluation sécurisée d'une fonction appliquée à des signaux cryptés

Publication

EP 2278750 A1 20110126 (EN)

Application

EP 10006107 A 20100611

Priority

US 49572109 A 20090630

Abstract (en)

Embodiments of the invention describe a system and a method for determining securely a result of applying a function to a first encrypted signal and a second encrypted signal resulted from encrypting a first signal and a second signal respectively, The method expresses the function as a linear combination of homomorphic components, wherein a homomorphic component is an algebraic combination of the first signals and the second signal such that an encrypted result of the algebraic combination is suitable to be calculated directly from the first encrypted signal and the second encrypted signal using homomorphic properties. Next, the method determines encrypted results of the homomorphic components from the first encrypted signal and the second encrypted signal, and combines the encrypted results of the homomorphic components according to the linear combination to produce the encrypted result of the function. The method is executed by a plurality of processors.

IPC 8 full level

H04L 9/00 (2006.01)

CPC (source: EP US)

H04L 9/008 (2013.01 - EP US); **H04L 9/3231** (2013.01 - EP US); H04L 2209/46 (2013.01 - EP US)

Citation (applicant)

US 52930410 A

Citation (search report)

- [I] WO 2006054208 A1 20060526 - KONINKL PHILIPS ELECTRONICS NV [NL], et al
- [A] WO 2005043808 A1 20050512 - KONINKL PHILIPS ELECTRONICS NV [NL], et al
- [A] BART GOETHALS ET AL: "On Private Scalar Product Computation for Privacy-Preserving Data Mining", 24 May 2005, INFORMATION SECURITY AND CRYPTOLOGY Â ICISC 2004; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/ HEIDELBERG, PAGE(S) 104 - 120, ISBN: 978-3-540-26226-8, XP019010724

Cited by

EP2293492A3; EP2680488A4; CN105052070A; EP4049403A4; US8966277B2; WO2014142042A1

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

Designated extension state (EPC)

BA ME RS

DOCDB simple family (publication)

US 2010329448 A1 20101230; CN 101938463 A 20110105; EP 2278750 A1 20110126; JP 2011013672 A 20110120

DOCDB simple family (application)

US 49572109 A 20090630; CN 201010220255 A 20100630; EP 10006107 A 20100611; JP 2010127478 A 20100603